

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 1-48. (Cancelled)

1 49. (New) A method for managing a database system, comprising:
2 receiving a command to perform an administrative function involving a
3 user within the database system;
4 determining if the user is a sensitive user who is empowered to access
5 sensitive data in the database system;
6 if the user is not a sensitive user, and if the command is received from a
7 normal database administrator for the database system, allowing the
8 administrative function to proceed;
9 if the user is a sensitive user, and if the command is received from a
10 normal administrator, disallowing the administrative function; and
11 if the user is a sensitive user, and if the command is received from a
12 security officer who is empowered to perform administrative functions for
13 sensitive users, allowing the administrative function to proceed.

1 50. (New) The method of claim 49, further comprising:
2 receiving a request to perform an operation on a data item in the database
3 system;
4 if the data item is a sensitive data item containing sensitive information
5 and if the request is received from a sensitive user who is empowered to access
6 sensitive data, allowing the operation to proceed if the sensitive user has access
7 rights to the sensitive data item; and

8 if the data item is a sensitive data item and the request is received from a
9 user who is not a sensitive user, disallowing the operation.

1 51. (New) The method of claim 50, wherein if the data item is a
2 sensitive data item, if the operation is allowed to proceed, and if the operation
3 involves retrieval of the data item, the method further comprises decrypting the
4 data item using an encryption key after the data item is retrieved.

1 52. (New) The method of claim 51, wherein the encryption key is
2 stored along with a table containing the data item.

1 53. (New) The method of claim 52, wherein the encryption key is
2 stored in encrypted form.

1 54. (New) The method of claim 49, wherein if the user is not a
2 sensitive user, and if the command to perform the administrative function is
3 received from a security officer, the method further comprises allowing the
4 security officer to perform the administrative function on the user.

1 55. (New) A computer-readable storage medium storing instructions
2 that when executed by a computer cause the computer to perform a method for
3 managing a database system, the method comprising:

4 receiving a command to perform an administrative function involving a
5 user within the database system;

6 determining if the user is a sensitive user who is empowered to access
7 sensitive data in the database system;

8 if the user is not a sensitive user, and if the command is received from a
9 normal database administrator for the database system, allowing the
10 administrative function to proceed;

11 if the user is a sensitive user, and if the command is received from a
12 normal administrator, disallowing the administrative function; and

13 if the user is a sensitive user, and if the command is received from a
14 security officer who is empowered to perform administrative functions for
15 sensitive users, allowing the administrative function to proceed.

1 56. (New) The computer-readable storage medium of claim 55,
2 wherein the method further comprises:

3 receiving a request to perform an operation on a data item in the database
4 system;

5 if the data item is a sensitive data item containing sensitive information
6 and if the request is received from a sensitive user who is empowered to access
7 sensitive data, allowing the operation to proceed if the sensitive user has access
8 rights to the sensitive data item; and

9 if the data item is a sensitive data item and the request is received from a
10 user who is not a sensitive user, disallowing the operation.

1 57. (New) The computer-readable storage medium of claim 56,
2 wherein if the data item is a sensitive data item, if the operation is allowed to
3 proceed, and if the operation involves retrieval of the data item, the method
4 further comprises decrypting the data item using an encryption key after the data
5 item is retrieved.

1 58. (New) The computer-readable storage medium of claim 57,
2 wherein the encryption key is stored along with a table containing the data item.

1 59. (New) The computer-readable storage medium of claim 58,
2 wherein the encryption key is stored in encrypted form.

1 60. (New) The computer-readable storage medium of claim 55,
2 wherein if the user is not a sensitive user, and if the command to perform the
3 administrative function is received from a security officer, the method further
4 comprises allowing the security officer to perform the administrative function on
5 the user.

1 61. (New) An apparatus that manages a database system, comprising:
2 a command-receiving mechanism configured to receive a command to
3 perform an administrative function involving a user within the database system;
4 an execution mechanism configured to,
5 determine if the user is a sensitive user who is empowered
6 to access sensitive data in the database system;
7 allow the administrative function to proceed, if the user is
8 not a sensitive user, and if the command is received from a normal
9 database administrator for the database system;
10 disallow the administrative function, if the user is a
11 sensitive user, and if the command is received from a normal
12 administrator; and to
13 allow the administrative function to proceed, if the user is a
14 sensitive user, and if the command is received from a security

15 officer who is empowered to perform administrative functions for
16 sensitive users.

1 62. (New) The apparatus of claim 17,
2 wherein the command-receiving mechanism is configured to receive a
3 request to perform an operation on a data item in the database system;
4 wherein the execution mechanism is configured to,
5 allow the operation to proceed, if the data item is a
6 sensitive data item containing sensitive information and if the
7 request is received from a sensitive user who is empowered to
8 access sensitive data, and if the sensitive user has access rights to
9 the sensitive data item; and to
10 disallowing the operation, if the data item is a sensitive data
11 item, and the request is received from a user who is not a sensitive
12 user.

1 63. (New) The apparatus of claim 18, further comprising a decryption
2 mechanism, wherein if the data item is a sensitive data item, if the operation is
3 allowed to proceed, and if the operation involves retrieval of the data item, the
4 decryption mechanism is configured to decrypt the data item using an encryption
5 key after the data item is retrieved

1 64. (New) The apparatus of claim 19, wherein the encryption key is
2 stored along with a table containing the data item.

1 65. (New) The apparatus of claim 20, wherein the encryption key is
2 stored in encrypted form.

1 66. (New) The apparatus of claim 17, wherein if the user is not a
2 sensitive user, and if the command to perform the administrative function is
3 received from a security officer, the execution mechanism is configured to allow
4 the security officer to perform the administrative function on the user.